REMARKS

The foregoing Amendment and the following Remarks are submitted in response to the Office Action issued on March 25, 2004 (Paper No. 5) in connection with the above-identified application, and are being filed within the three-month shortened statutory period set for a response by the Office Action.

Claims 1-4, 6-8, 10-15, 17-20, 22-27, 29-31, and 33-38, 40-43, 45, and 46 are pending in the present application, as amended. Claims 5 and 9 have been canceled and the subject matter thereof has been incorporated into claim 1, claims 28 and 32 have been canceled and the subject matter thereof has been incorporated into claim 24, claims 16, 21, 39, and 43 have been canceled and the subject matter thereof has been incorporated into claims 14, 19, 37, and 42, respectively, and claims depending from now-canceled claims have been amended to adjust dependencies. Applicants respectfully submit that no new matter has been added to the application by the Amendment.

The Examiner has rejected claims 1-4 and 24-27 under 35 USC § 102(e) as being anticipated by England et al. (U.S. Patent No. 6,330,670), and has also rejected claims 5-10 and 28-33 under 35 USC § 103(a) as being obvious over the England reference. Inasmuch as independent claims 1 and 24 have been amended to include the subject matter of claims 5 and 9 and 28 and 32, respectively, Applicants will address the rejections of the independent claims in terms of the rejections of claims 9 and 32. That said, Applicants respectfully traverse the England rejections.

Independent claim 1 as amended recites a method for enabling the rendering of digital content on a device, such as for example a portable player. In the method, the content is transferred to the device, such as for example from a coupled-to computing device, and a digital license corresponding to the content is obtained, again for example by the computing device. A sub-license corresponding to and based on the obtained license is composed, again for example by the computing device, and is transferred to the device. The sub-license enables rendering of the content on the device only in accordance with the terms thereof.

In the method, the content is encrypted and decryptable according to a content key and the license includes the content key encrypted into a form un-decryptable by the device. Composing the sub-license, then, includes re-encrypting the content key into a form that is decryptable by the device, and placing the re-encrypted content key in the sub-license. In addition, composing the sub-license includes placing indexing information in the sub-license, where the indexing information identifies a secret to the device that the device employs to decrypt the encrypted content key.

Independent claim 28 recites substantially the same subject matter as independent claim 1, although in the form of a computer-readable medium with computer-executable instructions for performing the method of claim 1.

As set forth in the specification of the present application, the secret may be a symmetric key that is shared between the computing device and the portable device, and is employed to encrypt the content key (KD) within the sub-license for such portable device to result in (SECRET(KD)). The shared (SECRET) must be derivable by both the portable device and the computing device. In particular, the shared (SECRET) is a function of the content ID of the content, and an identifier that identifies the portable device. However, such items are readily available to anyone, including any nefarious entity wishing to render the content without benefit of any license or sub-license. Accordingly, in one embodiment of the present invention, the shared (SECRET) is additionally a function of a shared (SUPER-SECRET) that is derivable by both the portable device and the computing device:

(SECRET) = function (content ID, portable device identifier, (SUPER-SECRET)).

Note, though, that inasmuch as the shared (SUPER-SECRET) may be a universal super-secret, such a universal super-secret would eventually become public. Accordingly, in one embodiment of the present invention, the shared (SUPER-SECRET) is a function of a (SUPER-SUPER-SECRET) and an indexing value j:

(SUPER-SECRET) = function ((SUPER-SUPER-SECRET), j).

Thus, a no-longer-trustworthy (SUPER-SECRET) may be replaced merely by incrementing the indexing value j and deriving a new (SUPER-SECRET) via the function and (SUPER-SUPER-SECRET).

Note that another layer of protection may be provided in the event (SUPER-SUPER-SECRET) does in fact become compromised. In particular, in such case, (SUPER-SUPER-SECRET) is provided with an indexing value k, where such indexing value k is incremented each time a new (SUPER-SUPER-SECRET) is put into use. As may be appreciated, then, the shared (SUPER-SECRET) is a function of a particular (SUPER-SUPER-SECRET) as indexed by the indexing value k, the aforementioned indexing value j, and also the indexing value k itself:

(SUPER-SECRET) = function ((SUPER-SUPER-SECRET), j, k).

The England reference discloses a digital rights management (DRM) system wherein content may be sub-licensed from a first computing device to a second, and where the sub-license for the second computing device to render the content includes a content decryption key encrypted according to a key available to such second computing device. However, and significantly, the England reference does not disclose, teach , or suggest that composing the sub-license includes placing indexing information in the sub-license, where the indexing information identifies a secret that the second computing device employs to decrypt the encrypted content key, as is now required by claims 1 and 24 as amended. In fact, the England reference does not at all appear to recognize that a secret shared between the first and second computing devices should be identified within a sub-license, or that such identification may occur by way of indexing information which can be employed to derive the secret.

Accordingly, Applicants respectfully submit that the England reference cannot be applied to make obvious claims 1 or 24 or any claims depending therefrom. As a result, Applicants respectfully request reconsideration and withdrawal of the England rejections.

The Examiner has rejected claims 11-13 and 34-36 under 35 USC § 103(a) as being obvious over Down et al. (U.S. Patent No. 6,574,609). Applicants respectfully traverse the Downs rejection.

Independent claim 11 recites a method for rendering digital content on a device. In the method, the content is received onto the device, in a form where the content encrypted and decryptable according to a content key. A digital license corresponding to the content is also received onto the device, where the license includes the content key encrypted and decryptable according to a secret. As above, the license also includes indexing information identifying the secret to the device. Thus, the indexing information in the license is obtained to identify the secret, and the secret is acquired based at least in part on the indexing information. Thereafter, the secret may be applied to the encrypted content key to decrypt and obtain the content key, and the obtained content key may be applied to the encrypted content to decrypt and obtain the content.

Independent claim 34 recites substantially the same subject matter as independent claim 11, although in the form of a computer-readable medium with computer-executable instructions for performing the method of claim 11.

The Downs reference discloses a DRM system wherein content is rendered in accordance with a corresponding license. However, and as the Examiner concedes, the Downs reference does not disclose a license with indexing information identifying a secret by which a content key may be decrypted. Nevertheless, the Examiner concludes that such a license with indexing information would be obvious based on a mention in the Downs reference at column 71, lines 50-53, that an offer SC may be created and stored within an offer database in an indexed manner according to a product ID. Applicants respectfully submit that such mention in the Downs reference has nothing to do with any Downs license, and does not at all disclose, teach, or suggest that a license should or could be provided with indexing information that identifies a secret by which a content key may be decrypted, as is required by claims 11 and 34.

Accordingly, Applicants respectfully submit that such mention cannot be employed in connection with the Downs reference to make obvious claims 11 or 34 or any claims depending therefrom. As a result, Applicants respectfully request reconsideration and withdrawal of the Downs rejection.

The Examiner has rejected claims 14-23 and 37-46 under 35 USC § 103(a) as being obvious over Matias et al. (U.S. Patent No. 6,681,017). Applicants respectfully traverse the Matias rejection.

Independent claim 14 recites a method for composing a license for rendering digital content on a device, where the content is encrypted and decryptable according to a content key. In the method, a secret is derived by obtaining a device identifier, acquiring a super-secret that is also acquirable by the device, and applying the obtained device identifier and super-secret to a function to derive the secret:

(SECRET) = function (device identifier, (SUPER-SECRET));

Thereafter, the content key is encrypted according to the derived secret such that the content key is decryptable according to the secret, and the encrypted content key is placed in the license. Significantly, the super-secret is identified by indexing information, and the method further comprises placing the indexing information in the license, whereby the device may obtain the indexing information from the license and thereby identify the super-secret by way of the indexing information.

Independent claim 19 recites a method for rendering digital content on a device, where the content is encrypted and decryptable according to a content key that is in turn encrypted and decryptable according to a secret. In the method, the encrypted content key is obtained from a digital license corresponding to the content such as that which is produced by the method of claim 14, and the secret is again derived in the manner of claim 14. The content key is then decrypted according to the derived secret and the content is decrypted according to the derived content key and rendered.

Independent claims 37 and 42 recite substantially the same subject matter as independent claims 14 and 19, respectively, although in the form of a computer-readable medium with computer-executable instructions for performing the methods.

The Matias reference discloses a Janus function J to derive shared keys, particularly at column 5, line 48 through column 6, line 13. As seen, the Janus function J receives as inputs a device identifier, a client identifier, and a secret. However, and significantly, the Janus function does not employ a super-secret that is identified by indexing information, as is required by claims 14, 19, 37, and 42. Accordingly, the Matias reference does not disclose, teach, or suggest by way of such Janus function J that the indexing information be in a license and be obtained therefrom to identify the super-secret by way of the indexing information, all as required by claims 14, 19, 37, and 42.

Applicants take note that the Examiner has taken Official Notice that such indexing information may be so stored and obtained. However, Applicants respectfully point out that although the Examiner may take Official Notice of facts outside of the record which are capable of instant and unquestionable demonstration as being "well-known" in the art, the facts so noticed serve to 'fill the gaps' which might exist in the evidentiary showing" and should not comprise the principle evidence upon which a rejection is based. See MPEP 2144.03.

Applicants respectfully submit here that the Examiner has impermissibly taken Official Notice of facts which comprise the principal evidence upon which the Matias rejection is based. In particular, Applicants respectfully submit that 'identifying the secret key by indexing information' is the critical missing piece in the Matias reference, and is not merely a 'gap' in the evidentiary showing that must be filled. Put another way, Applicants respectfully submit that the Examiner has impermissibly taken Official Notice of that element which is so clearly missing from the Matias reference, where such element is central to the rejection of the claims, and is not merely incidental to the rejection. As a result, Applicants respectfully request that the Examiner withdraw the taking of Official Notice in connection with the Matias rejection.

Accordingly, Applicants respectfully submit that such Matias reference cannot be applied to make obvious claims 14, 19, 37, or 42 or any claims depending therefrom. As a result, Applicants respectfully request reconsideration and withdrawal of the Matias rejection.

In view of the foregoing Amendment and Remarks, Applicants respectfully submit that the present application including claims 1-4, 6-8, 10-15, 17-20, 22-27, 29-31, and 33-38, 40-43, 45, and 46 is in condition for allowance and such action is respectfully requested.

Respectfully submitted,

Date: June 24, 2004

Steven H. Meyer
Registration No. 37,189

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439